09/601363
PCT/DE 99/03554
#3
5 Jan 01
R. Talbot

BUNDESREPUBLIK DEUTSCHLAND

DE 99/3554

EJV

Bescheinigung

Die ORGA Consult GmbH in Paderborn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Tragbarer mikroprozessorgestützter Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist"

am 2. Dezember 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 07 F 7/08 der Internationalen Patentklassifikation erhalten.

München, den 17. Dezember 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hoiß

Aktenzeichen 198 55 596.2

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

A 9161
06.90
11/98

Zusammenfassung

Titel: Tragbarer mikroprozessorgestützter Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist

Beschrieben ist ein tragbarer, mikroprozessorgestützter Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist.

Dabei ist in dem tragbaren Datenträger für mindestens einen Speicherbereich mindestens eine datenübertragungsspezifische Zugriffsbedingung gespeichert ist, die in Abhängigkeit von der Art der Datenübertragung (kontaktlos bzw. kontaktbehaftet) zwischen dem tragbaren Datenträger und einem Dateneingabe-/Datenausgabegerät die Bedingung definiert, unter der der Zugriff auf bestimmte Speicherbereiche erlaubt ist.

Titel: Tragbarer mikroprozessorgestützter Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist

Die Erfindung bezieht sich auf einen tragbaren, mikroprozessorgestützten Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist. Dabei ist der tragbare Datenträger vorzugsweise als Chipkarte ausgebildet.

Kontaktbehaftete Karten verfügen über elektrische Kontaktflächen für die Energieversorgung und den Datenaustausch mit einem entsprechenden im Berührungskontakt kontaktbehaftet arbeitenden Dateneingabe-/Datenausgabegerät. Kontaktbehaftete Karten sind seit längerer Zeit als Zugangsberechtigungskarten für GSM-Mobilfunksysteme, Telefonkarten, Krankenversichertenkarten, Bankkarten etc.weit verbreitet.

Kontaktlose Karten enthalten eine Spule als Antenne für die Energieversorgung und den Datenaustausch mit einem entsprechenden kontaktlos (induktiv) arbeitenden Dateneingabe-/Datenausgabegerät. Dabei ist in der Karte ein Antennen-Interface vorgesehen, das aus einer in der Spule induzierten Wechselspannung eine Gleichspannung zur Spannungsversorgung des Mikroprozessors erzeugt. Das Antennen-Interface dient auch als Signalumformer für die zwischen dem kontaktlos arbeitenden Terminal und dem Mikroprozessor auszutauschenden Daten. Das Antennen-Interface ist vorzugsweise gemeinsam mit dem Mikroprozessor auf einem Halbleiterbaustein integriert.

Gegenstand der Erfindung ist ein tragbarer, mikroprozessorgestützter Datenträger, der beide Funktionalitäten (kontaktbehaftet und kontaktlos) in sich vereint. Derartige tragbare

Datenträger sind unter den Begriffen Combicard (Kombination der kontaktbehafteten und der kontatklosen Funktionalität) oder Dual-Interface-Card (Karte mit kontaktbehafteter und kontaktloser Schnittstelle) bekannt.

Die Art der Datenübertragung zwischen dem tragbaren Datenträger und einem kontaktbehaftet arbeitenden Dateneingabe-/Datenausgabegerät ist naturgemäß von der Art der Datenübertragung zwischen dem tragbaren Datenträger und einem kontaktlos arbeitenden Dateneingabe-/Datenausgabegerät verschieden. Für den kontaktbehafteten Betrieb und für den kontaktlosen Betrieb des tragbaren Datenträgers werden verschiedene Übertragungsprotokolle verwendet. Selbst nur für den kontaktbehafteten Betrieb sind verschiedene Übertragungsprotokolle (T=0, T=1,T=14) bekannt.

Die tragbaren Datenträger, die Gegenstand der Erfindung sind, unterstützen dabei sowohl mindestens ein Übertragungsprotokoll für den kontaktbehafteten Betrieb (z.B. T= 1) als auch ein Übertragungsprotokoll für den kontaktlosen Betrieb.

Die erfindungsgegenständlichen tragbaren Datenträger verfügen über ein Betriebssystem, das - unabhängig von der Art der Datenübertragung - die in verschiedenen Speicherbereichen gespeicherten Daten entsprechend der von dem jeweiligen Dateneingabe-/Datenausgabegerät erhaltenen Kommandos bearbeitet und verwaltet.

Auf so einem Betriebssystem können nun wiederum ein, zwei oder mehrere Applikationsprogramme installiert sein. Derartige tragbare Datenträger, auf denen mehrere Applikationsprogramme installiert sind, werden auch als multifunktionale Chipkarten bezeichnet. Bei dem erfindungsgegenständlichen tragbaren Datenträger würde man dann von einer multifunktionalen Dual-Interface-Karte sprechen. Jeder Applikation können dabei verschiedene Speicherbereiche zugeordnet sein. So könnte der tragbare Datenträger bspw. eine von Banken beaufsichtigte Geldkarten-Applikation und eine von einem öffentlichen Personennahverkehrsnetz-Betreiber beaufsichtige ÖPNV-Applikation umfassen. Dabei wäre der Geldkarten-Applikation als Speicherbereich eine Geldbörse zugeordnet und der ÖPNV-Applikation als Speicherbereich eine entsprechende ÖPNV-Börse zugeordnet.

Während die kontaktbehaftete Verwendung des tragbaren Datenträgers immer voraussetzt, daß der Inhaber des tragbaren Datenträgers diesen bewußt, willentlich in das entsprechende

Dateneingabe-/Datenausgabegerät einführt, ist dieses bewußte, willentliche Vorgehen im kontaktlosen Fall für das Zustandekommen einer Datenübertragung nicht immer notwendig. Aufgrund der zum Teil relativ großen Reichweite der kontaktlos arbeitenden Dateneingabe-/Datenausgabegeräte kann eine Datenübertragung auch schon erfolgen, wenn der tragbare Datenträger sich z.B. noch in einer Tasche des Datenträgerinhabers befindet. So kann z.B. jedesmal automatisch beim Durchqueren des Eingangs- und/oder Ausgangsbereiches von U-Bahnstationen eine kontaktlose Datenübertragung zwecks einer schnellen und bequemen Fahrpreisbezahlung aufgebaut werden.

Dieser Vorteil der kontaktlosen Betriebsweise stellt jedoch bei einem tragbaren Datenträger, der sowohl kontaktlos als auch kontaktbehaftet betrieben werden kann, ein Risiko dar. Dieses Risiko besteht nun darin, daß Angreifer versuchen könnten, über ein kontaktlos arbeitendes Dateneingabe-/Datenausgabegerät unbemerkt auch auf Speicherbereiche zuzugreifen, die eigentlich der kontaktbehafteten Applikation vorbehalten sind, wobei der Zugriff auf diese Speicherbereich normalerweise das bewußte, willentliche Einführen des Datenträgers in das kontaktbehaftet arbeitende Dateneingabe-/Datenausgabegerät voraussetzt.

Aufgabe der Erfindung ist es daher, einen tragbaren, mikroprozessorgestützten Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist, zu schaffen, bei dem sichergestellt ist, daß ein für den Inhaber des Datenträgers unbewußter kontaktloser Zugriff auf Speicherbereiche, die der kontaktbehafteten Applikation vorbehalten sein sollen, nicht möglich ist.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß in dem tragbaren Datenträger für mindestens einen Speicherbereich mindestens eine datenübertragungsspezifische Zugriffsbedingung gespeichert ist, die in Abhängigkeit von der Art der Datenübertragung zwischen dem tragbaren Datenträger und einem Dateneingabe-/Datenausgabegerät die Bedingung definiert, unter der der Zugriff auf diesen Speicherbereich erlaubt ist.

Die Zugriffsbedingung kann ein einzelnes Bit sein, das als Flag anzeigt, ob der Zugriff bei der aktuellen Art der Datenübertragung (kontaktbehaftet oder kontaktlos) auf diesen Speicherbereich erlaubt ist oder nicht.

aktiven kontaktbehafteten Übertragungsprotokoll (T=0, T=1, T=14) die Bedingung definiert, unter der der Zugriff auf einen Speicherbereich erlaubt ist.

Die erfindungsgemäße datenübertragungsspezifische Zugriffsbedingung ist dabei von autorisierten Stellen unter Verwendung einer Geheiminformation in einen frei programmierbaren, nichtflüchtigen Speicher des tragbaren Datenträgers eingebbar, vorzugsweise können die Zugriffsbedingungen auch umprogrammiert werden. Die Programmierung der Zugriffsbedingungen erfolgt in sogenannten Initialisierungs- und/oder Personalisierungsschritten.

Anstatt die Zugriffsbedingungen frei zu programmieren, können diese auch in einem nicht änderbaren Festwertspeicher (ROM) gespeichert sein.

Anhand der beigefügten Zeichnungen soll die Erfindung nachfolgend näher erläutert werden.

Figur 1 zeigt den in Form einer Chipkarte ausgebildeten tragbaren Datenträger. Für die kontaktbehaftete Betriebsweise weist dieser auf einer Kartenseite elektrisch leitende Kontaktflächen (Ki) auf. Für die kontaktlose Betriebsweise befindet sich in dem Kartenkörper eine Antenne (A) in Form einer Spule. Zur Veranschaulichung ist der Kartenkörper im Bereich der Spulenwicklung an zwei Stellen aufgebrochen dargestellt.

Figur 2 zeigt eine schematische Darstellung des tragbaren Datenträgers. Dargestellt ist der Halbleiterbaustein mit Mikroprozessor, Speicher und integriertem Antennen-Interface. An diesen einen Halbleiterbaustein ist einerseits die Antenne (A) über entsprechende Anschlußleitungen (LA) angeschlossen und andererseits die Kontaktflächen (Ki) über entsprechende Anschlußleitungen (LKi). In dem Halbleiterbaustein befindet sich neben der CPU als zentraler Recheneinheit ein Festwertspeicher (ROM), in dem zumindest Teile des Betriebssystems abgelegt sind, und ein flüchtiger Arbeitsspeicher (RAM). Daneben existiert ein in verschiedene Speicherbereiche eingeteilter nicht flüchtiger, programmierbarer Speicher (EEPROM). In diesem Speicher kann u.a. ein Teil des Betriebssystems gespeichert sein. Darüber hinaus befinden sich dort die Applikationsprogramme mit entsprechenden Speicherbereichen als Datenfelder.

Figur 3A zeigt den tragbaren Datenträger schematisch in Verbindung mit einem kontaktbehaftet arbeitenden Dateneingabe-/Datenausgabegerät; Figur 3B zeigt den tragbaren Datenträger schematisch in Verbindung mit einem kontaktlos arbeitenden Dateneingabe-/Datenausgabegerät.

In Figur 4 sind verschiedene Speicherbereiche des EEPROM-Speichers mit den entsprechenden erfindungsgemäßen Zugriffsbedingungen schematisch exemplarisch dargestellt. Dabei ist der i.Speicherbereich als Datenfeld für eine Geldbörse vorgesehen, die in Verbindung mit der kontaktbehafteten Geldkarten-Applikation betrieben verwendet wird. Daneben gibt es den j. Speicherbereich der als Datenfeld für eine weitere Börse dient, die in Verbindung mit der kontaktlosen ÖPNV-Applikation verwendet wird.
Dem Speicherbereich „Geldbörse“ sind dabei 4 Zugriffsbedingungen (ZB1, ZB2, ZB3, ZB4) zugeordnet, die den Zugriff auf diesen Speicherbereich in Abhängigkeit von der

kontaktbehafteten oder der kontaktlosen Betriebsweise definieren. Im einfachsten Fall sind die Zugriffsbedingungen als Flag in Form eines einzigen Bits, das gesetzt oder nicht gesetzt sein kann, gespeichert.

So bedeutet bspw.
ZB1 = 1 : Read-Command im kontaktbehafteten Betrieb erlaubt,
ZB1 = 0 : Read-Command im kontaktbehafteten Betrieb verboten,
ZB2 = 1 : Update-Command im kontaktbehafteten Betrieb erlaubt,
ZB2 = 0 : Update-Command im kontaktbehafteten Betrieb verboten,
ZB3 = 1 : Read-Command im kontaktlosen Betrieb verboten,
ZB3 = 0 : Read-Command im kontaktlosen Betrieb erlaubt,
ZB4 = 1 : Update-Command im kontaktlosen Betrieb verboten,
ZB2 = 0 : Update-Command im kontaktlosen Betrieb erlaubt.

Entsprechendes gilt für die Zugriffsbedingungen der ÖPNV-Börse.

Die Zugriffsbedingungen selbst sind intern (im tragbaren Datenträger) in beiden Betriebsmodi auslesbar. Optional können die Zugriffsbedingungen auch von den Dateneingabe-/Datenausgabegeräten ausgelesen werden. Änderbar sind sie jedoch nur von autorisierten Stellen.

Patentansprüche

1) Tragbarer, mikroprozessorgestützter Datenträger, der sowohl kontaktbehaftet als auch kontaktlos betreibbar ist, wobei
   - die Datenübertragung im kontaktbehafteten Betrieb zwischen dem tragbaren Datenträger und einem kontaktbehaftet arbeitenden Dateneingabe-/Datenausgabegerät erfolgt,
   - die Datenübertragung im kontaktlosen Betrieb zwischen dem tragbaren Datenträger und einem kontaktlos arbeitenden Dateneingabe-/Datenausgabegerät erfolgt,
   - der tragbare Datenträger mindestens einen in verschiedene Speicherbereiche aufgeteilten Speicher aufweist,
   - in dem tragbaren Datenträger für mindestens einen Speicherbereich mindestens eine Zugriffsbedingung gespeichert ist, die definiert unter welcher Bedingung der Zugriff auf diesen Speicherbereich erlaubt ist,

dadurch gekennzeichnet, daß

in dem tragbaren Datenträger für mindestens einen Speicherbereich mindestens eine datenübertragungsspezifische Zugriffsbedingung gespeichert ist, die in Abhängigkeit von der Art der Datenübertragung zwischen dem tragbaren Datenträger und einem Dateneingabe-/Datenausgabegerät die Bedingung definiert, unter der der Zugriff auf diesen Speicherbereich erlaubt ist.

2) Tragbarer, mikroprozessorgestützter Datenträger nach Anspruch 1,
dadurch gekennzeichnet, daß
für mindestens einen Speicherbereich eine datenübertragungsspezifische Zugriffsbedingung für den kontaktlosen Betrieb vorgesehen ist, die im kontaktlosen Betrieb des tragbaren Datenträgers jeglichen Zugriff (alle Zugriffsarten, Kommandos) auf diesen Speicherbereich verbietet.

3) Tragbarer, mikroprozessorgestützter Datenträger nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß
für mindestens einen Speicherbereich eine datenübertragungsspezifische Zugriffsbedingung für den kontaktlosen Betrieb vorgesehen ist, die im kontaktlosen Betrieb des tragbaren Datenträgers für mindestens zwei verschiedene Zugriffsarten jeweils unterschiedliche Bedingungen definiert, unter denen der Zugriff erlaubt ist.

4) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
verschiedenen Zugriffsarten für einen Speicherbereich unterschiedliche datenübertragungsspezifische Zugriffsbedingungen für den kontaktlosen Betrieb zugeordnet sind, die im kontaktlosen Betrieb des tragbaren Datenträgers für die jeweilige Zugriffsart die Bedingungen definieren, unter denen der Zugriff erlaubt ist.

5) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
für mindestens einen Speicherbereich eine datenübertragungsspezifische Zugriffsbedingung für den kontaktbehafteten Betrieb vorgesehen ist, die im kontaktbehafteten Betrieb des tragbaren Datenträgers jeglichen Zugriff auf diesen Speicherbereich verbietet.

6) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
für mindestens einen Speicherbereich eine datenübertragungsspezifische Zugriffsbedingung für den kontaktbehafteten Betrieb vorgesehen ist, die im kontaktbehafteten Betrieb des tragbaren Datenträgers für mindestens zwei verschiedene Zugriffsarten jeweils unterschiedliche Bedingungen definiert, unter denen der Zugriff erlaubt ist.

7) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
verschiedenen Zugriffsarten für einen Speicherbereich unterschiedliche datenübertragungsspezifische Zugriffsbedingungen für den kontaktbehafteten Betrieb zugeordnet sind, die im kontaktbehafteten Betrieb des tragbaren Datenträgers für die jeweilige Zugriffsart die Bedingungen definieren, unter denen der Zugriff erlaubt ist.

8) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
für mindestens einen Speicherbereich für mindestens eine Zugriffsart eine datenübertragungsspezifische Zugriffsbedingung für den kontaktbehafteten Betrieb und eine datenübertragungsspezifische Zugriffsbedingung für den kontaktlosen Betrieb vorgesehen ist.

9) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
derselbe so ausgebildet ist, daß die datenübertragungsspezifische Zugriffsbedingung von autorisierten Stellen unter Verwendung einer Geheiminformation in einen frei programmierbaren, nicht flüchtigen Speicher des tragbaren Datenträgers eingebbar ist.

10) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß
derselbe so ausgebildet ist, daß die datenübertragungsspezifische Zugriffsbedingung von autorisierten Stellen unter Verwendung einer Geheiminformation in den tragbaren Datenträger umprogrammierbar ist.

11) Tragbarer, mikroprozessorgestützter Datenträger nach einem der vorstehenden Ansprüche 1 bis 8,
dadurch gekennzeichnet, daß
die datenübertragungsspezifische Zugriffsbedingung in einem nicht änderbaren Festwertspeicher des tragbaren Datenträgers gespeichert ist.

12) Verfahren zur Durchführung der Kommunikation zwischen einem tragbaren, mikroprozessorgestützten Datenträger und einem kontaktbehaftet arbeitenden Dateneingabe-/Datenausgabegerät oder einem kontaktlos arbeitenden Dateneingabe-/Datenausgabegerät, wobei

- der tragbare Datenträger mindestens einen in verschiedene Speicherbereiche aufgeteilten Speicher aufweist,
- in dem tragbaren Datenträger für mindestens einen Speicherbereich mindestens eine datenübertragungsspezifische Zugriffsbedingung gespeichert ist, die in Abhängigkeit von der Art der Datenübertragung zwischen dem tragbaren Datenträger und einem Dateneingabe-/Datenausgabegerät die Bedingung definiert, unter der ein Zugriff auf diesen Speicherbereich erlaubt ist,

dadurch gekennzeichnet, daß

vor dem Zugriff auf diesen Speicherbereich (Ausführung eines von dem Dateneingabe-/Datenausgabegerät gesendeten Zugriffskommandos) von dem tragbaren Datenträger selbst anhand eines in dem tragbaren Datenträger gespeicherten Kontrollprogramms die diesem Speicherbereich zugeordnete datenübertragungsspezifische Zugriffsbedingung ausgelesen wird und überprüft wird, ob im Fall der jeweils aktuellen Art der Datenübertragung das gewünschte Zugriffskommando unter Berücksichtigung der datenübertragungsspezifischen Zugriffsbedingung erlaubt ist, und nur dann, wenn die Kontrolle ergeben hat, daß der Zugriff erlaubt ist, das Zugriffskommando ausgeführt wird.

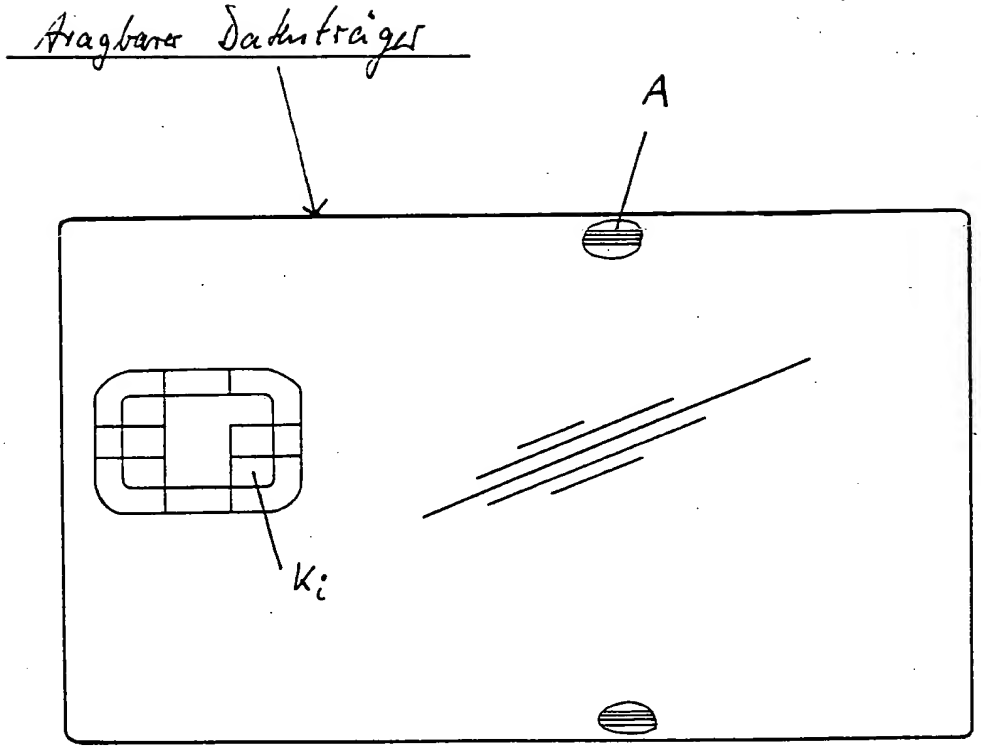


Fig. 1

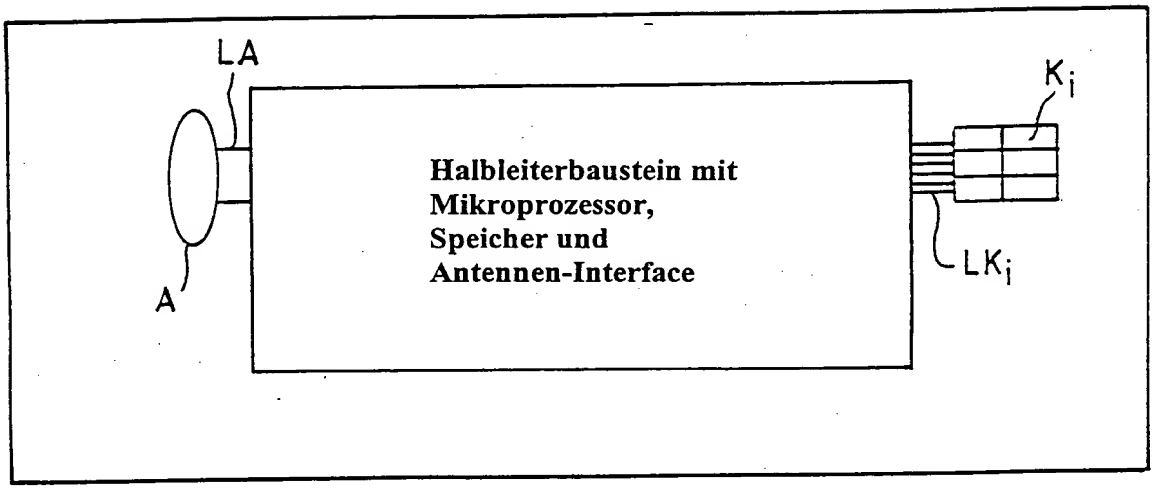

LA
A
Halbleiterbaustein mit
Mikroprozessor,
Speicher und
Antennen-Interface
Ki
LKi

Fig. 2

Fig. 3A

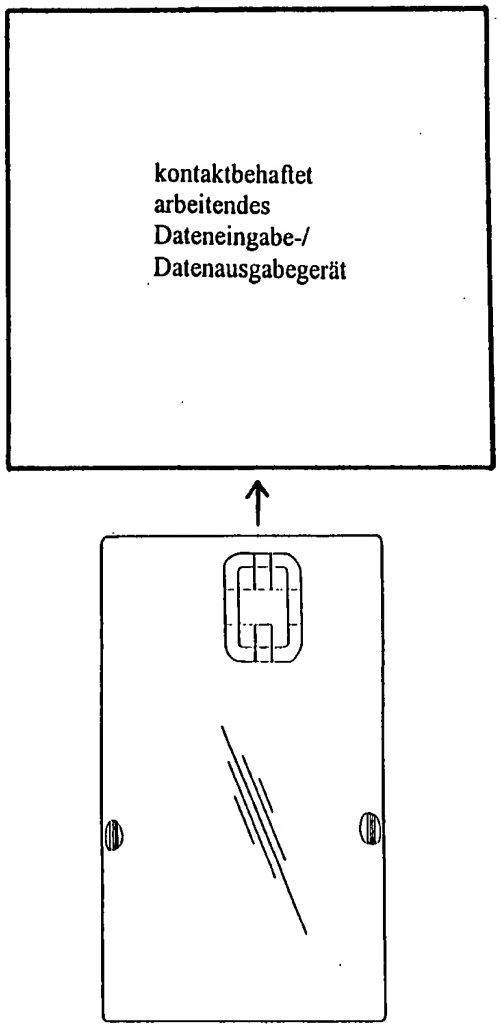
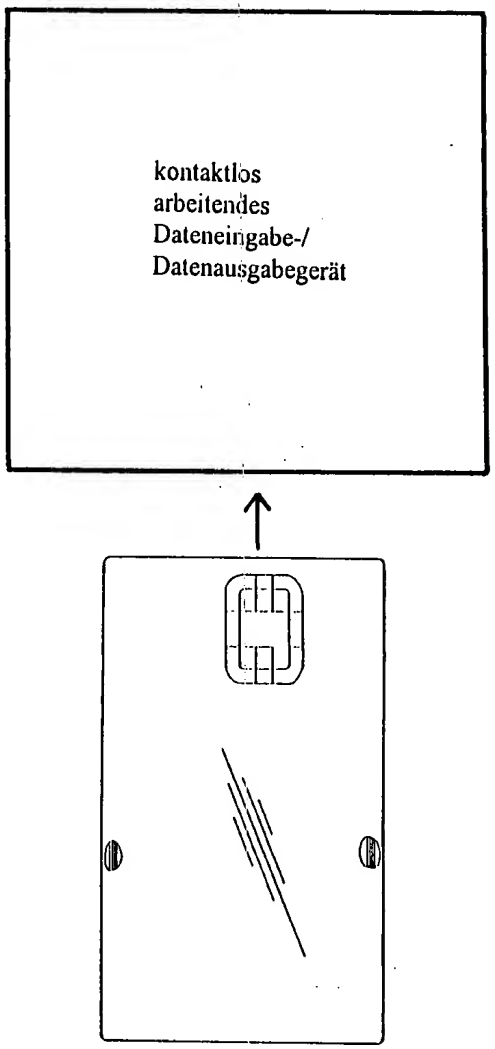

kontaktbehaftet
arbeitendes
Dateneingabe-/
Datenausgabegerät

Fig. 3B


kontaktlos
arbeitendes
Dateneingabe-/
Datenausgabegerät

EEPROM	
Zugriffsbedingungen	**1. Speicherbereich**
Zugriffsbedingungen	**2. Speicherbereich**
Zugriffsbedingungen	. . .
Zugriffsbedingungen ZB1 : Read-Command im kontaktbehafteten Betrieb erlaubt. ZB2 : Update-Command im kontaktbehafteten Betrieb erlaubt. ZB3 : Read-Command im kontaktlosen Betrieb verboten. ZB4 : Update-Command im kontaktlosen Betrieb verboten.	**i. Speicherbereich** **Geldbörse**
Zugriffsbedingungen ZB1 : Read-Command im kontaktbehafteten Betrieb erlaubt. ZB2 : Update-Command im kontaktbehafteten Betrieb erlaubt. ZB3 : Read-Command im kontaktlosen Betrieb erlaubt. ZB4 : Update-Command im kontaktlosen Betrieb erlaubt.	**j. Speicherbereich** **Börse für den öffentlichen Nahverkehr**
Zugriffsbedingungen	. .

Fig. 4